

الگوریتم‌های رمزنگاری

و

نفوذ در شبکه

دکتر سید نورالله والی

استاد دانشگاه آزاد اسلامی

واحد تهران شرق

۱۳۹۴

بسم الله الرحمن الرحيم

سرشناسه	: والہ، سید نورالہ، ۱۳۲۹ -
عنوان و نام پدید آور	: الگوریتم های رمز نگاری و نفوذ در شبکه /
مشخصات نشر	: تهران: سید نورالہ والہ، ۱۳۹۴.
مشخصات ظاہری	: ۱۵۰ص: مصور، جدول، نمودار.
شابک	: 978-600-04-4285-9
وضعیت فهرست نویسی	: فیبا
عنوان اصلی	: Coding Algorithms and Penetration in Network :
موضوع	: شبکه های کامپیوتری - - تدابیر ایمنی
موضوع	: آزمایش نفوذ - (ایمن سازی کامپیوتر)
موضوع	: کامپیوترها - ایمنی اطلاعات
موضوع	: الگوریتم های کامپیوتری
موضوع	: رمزنگاری
رده بندی کنگره	: ۱۳۹۴ الف ۷/۵۹/۵۱۰۵ TK
رده بندی دیویی	: ۰۵/۱۱
شماره کتابشناسی ملی	: ۲۲۱۰۰۹
نام کتاب	: الگوریتم های رمز نگاری و نفوذ در شبکه
تالیف	: دکتر سید نورالہ والہ
ناشر	: ناشر مولف دکتر سید نورالہ والہ
نوبت چاپ	: اول
چاپ	: مهدی
تیراژ	: ۵۰۰ نسخه
قیمت	: ۱۰۰,۰۰۰ ریال
تاریخ انتشار	: ۱۳۹۴
شابک	: ۹۷۸-۶۰۰-۰۴-۴۲۸۵-۹
* کلیه حقوق برای مؤلف محفوظ است.	

شابک: ۹۷۸-۶۰۰-۰۴-۴۲۸۵-۹

ISBN: 978-600-04-4285-9

تلفن: ۰۹۱۲۴۴۳۰۸۴۰ - ۸۸۲۵۴۳۰۰

رخنه کردن یا هک به معنی سود بردن از یک روش سریع و هوشمندانه برای حل یک مشکل در رایانه که رمزگشایی (crack) است نیز می‌باشد. در علوم مربوط به رایانه معنی هک گاه مساوی معنی کرک عنوان می‌شود. در گفتگوهای امروزی هک به معنی نفوذ به یک سیستم رایانه‌ای است و کرک نیز به معنی رمزگشایی است و کرکر به فرد گشاینده رمز می‌گویند.

گسترده‌گی واژه هک منحصر به رایانه نمی‌باشد و توسط افراد با تخصص‌های گوناگون در زمینه‌هایی از قبیل موسیقی، نقاشی و... نیز به کار می‌رود که به معنی دگرگونی‌های هوشمندانه و خلاقانه فرد در آن زمینه می‌باشد.

معنی اصلی آن سود بردن از یک روش سریع و هوشمندانه برای حل مشکلی تکنیکی بوده است. این واژه همواره با واژه مشتق شده دیگر آن هکر، به معنی کسی می‌باشد که توانایی پیاده سازی و ساخت یک‌های جدید را دارد. امنیت شبکه، به معنای حفاظت فیزیکی تنها نیست، بلکه یک مسئول امنیت شبکه باید بتواند از نظر سایبری نیز از آن دفاع کند و بابت بهره گیری از مسائل به سر آمده ریاضیات و منطق، همچنین نرم افزارهای جاسوسی و ضد جاسوسی معتبر و به روز باشد و بهره گیری از مسائل روز رمزنگاری و امضاهای دیجیتال، بتوانند از شبکه دفاع کامل کنند.

اگر به عنوان یک مشاور امنیتی، یک مسئول امنیت شبکه، یک مسئول شبکه و حتی یک کاربر خانگی پا به عرصه سایبری و دنیای پراز خطر و هیجان صفر و یک بگذارید بهتر است ابتدا با مسائل امنیتی آشنا شده، سپس علم خود را در این راستا افزایش دهید و با به روز رسانی مداوم علم خود، قدرت سایبری خود را به جهش‌های معرفتی نمایید. در مجموع شناخت الگوریتم‌های رمزنگاری به عنوان مهمترین عامل نرد در شبکه می‌باشد که در این مجموعه مورد بررسی قرار گرفته‌اند. امید است این مجموعه مؤثر و مفید واقع گردد.

دکتر سید نوراله واله

استاد دانشگاه آزاد اسلامی واحد تهران شرق

فصل اول

۹	کلیات شبکه
۹	مفاهیم امنیت شبکه
۱۵	امنیت فیزیکی - افزونگی در محل استقرار شبکه
۱۶	توپولوژی شبکه
۱۶	محل های امن برای تجهیزات
۱۷	انتخاب لایه ناخال ارتباطی امن
۱۸	منابع تعدیه
۱۹	عوامل محیطی
۱۹	امنیت منطقی
۱۹	امنیت مسیر یاب ها
۲۰	مدیریت پیکربندی
۲۱	کنترل دسترسی به تجهیزات
۲۱	امن سازی دسترسی
۲۲	مدیریت رمز های عبور
۲۲	ملزومات و مشکلات امنیتی ارائه دهندگان خدمات
۲۲	قابلیت های امنیتی
۲۴	الگوریتم رمز گذاری
۲۵	رمز های متقارن
۲۷	رمز نگاری نامتقارن
۳۰	یک طرفه الگوریتم هش
۳۱	هش چیست؟
۳۲	موارد استفاده از Hash ها
۳۲	انواع هش
۳۳	SSH چیست؟
۳۴	SSN

۳۴	رویکردی عملی به امنیت شبکه لایه بندی شده (۱).....
۳۶	افزودن به ضریب عملکرد هکرها.....
۳۷	سطح ۱: امنیت پیرامون.....
۳۷	تکنولوژیهای زیر امنیت را در پیرامون شبکه ایجاد می کنند:.....
۳۹	مزایا :.....
۳۹	معایب :.....
۳۹	ملاحظات :.....
۴۰	سطح ۲- امنیت شبکه.....
۴۱	مدیریت آسیب پذیری.....
۴۲	تابعیت امنیتی کاربر انتهایی.....
۴۳	کنترل دسترسی / باید.....
۴۳	مزایا :.....
۴۴	معایب :.....
۴۵	ملاحظات :.....
۴۶	رویکردی عملی به امنیت شبکه لایه بندی شده (۴).....
۴۶	سطح ۳- امنیت میزبان.....
۴۶	تکنولوژیهای زیر امنیت را در سطح میزبان فراهم می کنند:.....
۴۸	مزایا :.....
۴۸	معایب :.....
۴۹	ملاحظات :.....
۴۹	جمع بندی :.....
۴۹	دفاع در مقابل تهدیدها و حملات معمول :.....
۵۰	بعضی حملات معمول شامل موارد زیر می شود:.....
۵۱	پراکسی سرور:.....
۵۲	عملکردهایی که پراکسی سرور می تواند داشته باشد :.....
۵۵	کاربرد پراکسی در امنیت شبکه (۱).....
۵۵	پراکسی چیست؟.....
۵۶	پراکسی چه چیزی نیست؟.....
۵۶	پراکسی با Packet filter تفاوت دارد :.....

۵۷	پراکسی با Stateful packet filter تفاوت دارد
۵۸	پراکسی‌ها یا Application Gateways
۵۹	کاربرد پراکسی در امنیت شبکه (۲)
۶۰	برخی انواع پراکسی
۶۱	SMTP Proxy
۶۳	کاربرد پراکسی در امنیت شبکه (۳)
۶۳	HTTP Proxy
۶۵	FTP Proxy
۶۷	DNS Proxy
۶۸	مقایسه تشخیص نفوذ و پیش‌گیری از نفوذ
۶۹	تفاوت شکال تشخیص با پیش‌گیری
۶۹	تشخیص نفوذ
۷۱	پیش‌گیری از نفوذ

فصل دوم

۷۳	آشنایی با شبکه‌های کامپیوتری
۷۵	کاربرد شبکه‌های کامپیوتری
۷۵	اشتراک منابع
۷۵	حذف محدودیت‌های جغرافیایی در تبادل داده‌ها
۷۶	کاهش هزینه‌ها
۷۶	بالا رفتن قابلیت اعتماد سیستم‌ها
۷۶	افزایش کارایی سیستم
۷۷	انواع شبکه
۷۷	شبکه هم‌تا به هم‌تا
۷۸	شبکه مشتری - خدمت‌گزار
۷۹	مزایای شبکه‌های مشتری - خدمت‌گزار
۸۰	پروتکل‌های TCP / IP
۸۱	راهکارهای پروتکل TCP برای جبران کاستی‌های لایه IP
۸۲	انواع پورت‌های نرم افزاری
۸۴	مفهوم پورت‌های باز و بسته

۸۵	آشنایی با پورت‌های مختلف
۸۶	آدرس سخت افزاری:
۸۸	مبانی سرویس دهنده نام‌های حوزه
۹۰	نام دامنه
۹۲	نگاهی گذرا به سرویس دهندگان وب

فصل سوم

۹۵	آشنایی با نفوذ در شبکه
۹۶	تاریخچه نفوذ
۱۰۲	انگیزه نفوذگران: حمله به شبکه‌ها
۱۰۴	ریسک‌های مرتبط با افاد

فصل چهارم

۱۰۷	راه‌های نفوذ به شبکه
۱۰۸	نرم افزار Sam Spade
۱۱۲	حمله از طریق مودم
۱۱۴	حمله از طریق مودم‌های شبکه
۱۱۶	معرفی نرم افزار THC-Scan Version 2.0
۱۱۹	نرم افزار نقشه برداری از شبکه
۱۲۰	Firewalk علیه Firewall
۱۲۲	نرم افزار پسوردیاب PWDUM P2
۱۲۲	انواع هش
۱۲۴	ابزار تست وبسایت
۱۲۷	حمله از راه پشته
۱۳۰	کدهای سیاه
۱۳۷	درب‌های پستی
۱۴۲	اسب‌های تراول
۱۵۰	منابع و مآخذ